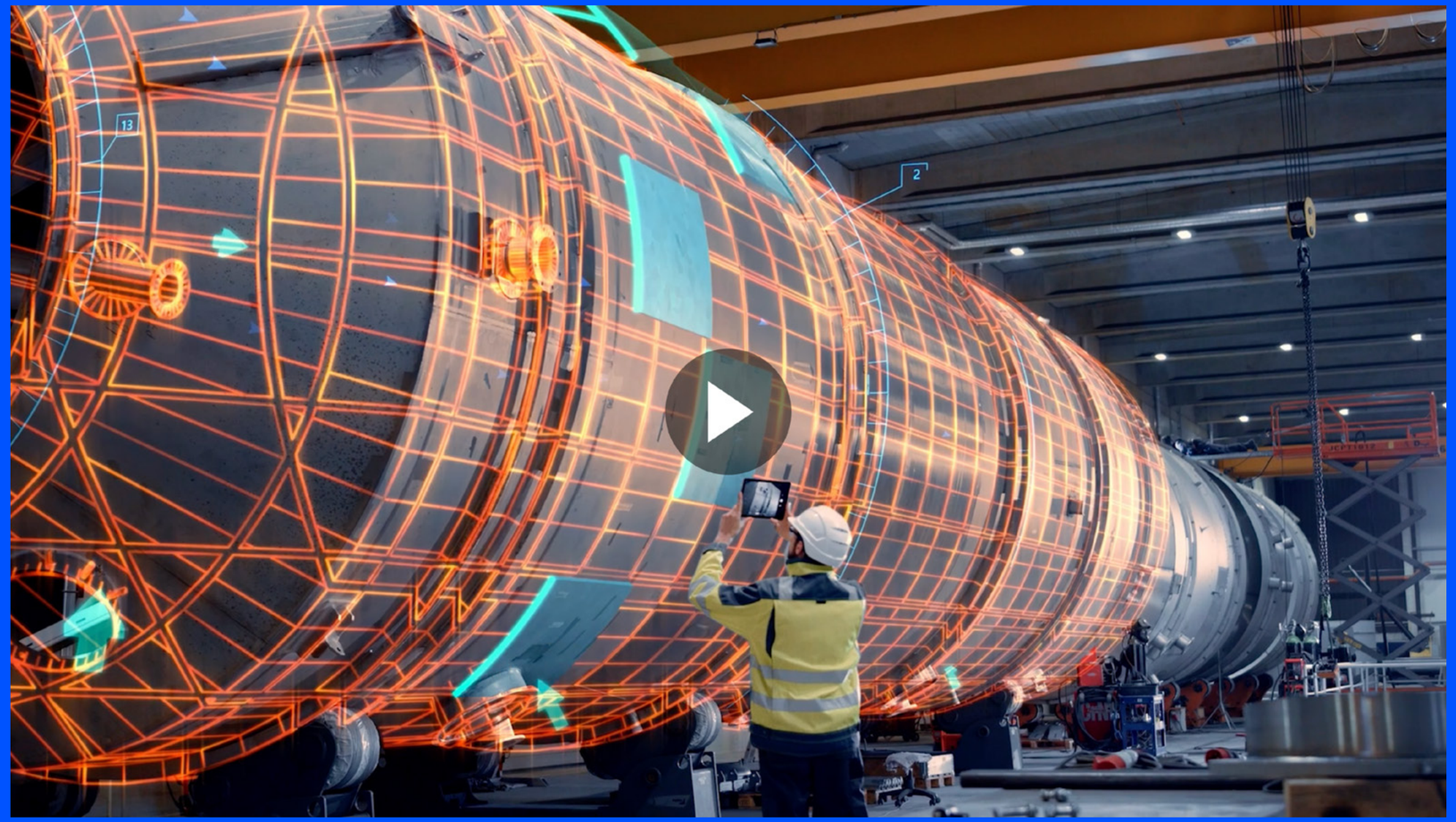
Getting smart about industry.

Navigating the path to industrial automation.

Navigating the path to industrial automation



Warren Jennings, CTO for Industry at Telstra and Alan Seery, Managing Director at Aqura introduce key considerations for industrial automation.

As Australia grapples with inflation, a tight labour market and supply chain challenges, forward-looking organisations are investing in automation to improve productivity, address the skills shortage and reduce operational costs.

The movement to automation-led business models doesn't just enable industries to streamline workflows, create efficiencies, improve flexibility and decision-making. Those models can also manage today's environmental, social and governance (ESG) requirements more easily by automating sustainability practices, environmental measurement, and safety monitoring and reporting.

A significant opportunity

The introduction of powerful new automation technologies such as robotics, sensors, machine-to-machine communications and edge computing, along with artificial intelligence (AI) approaches, such as machine learning (ML), has the potential to transform the Australian economy and enable us to compete into the future by boosting productivity and innovation.

We would like to acknowledge the valuable contributions of the following experts for their insights into industrial automation.

Warren Jennings
CTO for Industry
Telstra

Alan Seery
Managing
Director, Aqura

Matthew Griffiths
Managing
Director, Alliance
Automation

Gideon Ratner
Chief Customer
Officer, Quantium
Telstra

50-150%
predicted increase in average annual productivity growth in Australia through automation compared to baseline.[1]

$4-$15k
Additional annual income created by automation per Australian by 2030.[1]

30%
of Australian organisations are adopting automated solutions for sustainability and ESG reporting.[2]

25-46%
predicted percentage of existing Australian workforce activities that could be automated by 2030.[2]

According to Mckinsey, "If seized, this opportunity could add $1.1 trillion to $4 trillion to the economy over the next 15 years, providing every Australian with $4,000 to $15,000 in additional income per year by 2030."[1]

But while the appeal of industrial automation is clear, the process of getting there can be challenging.

Realising the true value of automation – safe, efficient operations with predictive capabilities and ultra-fast responsiveness – requires the ability to combine rich data from sensors and industrial systems and overlay it with data analytics. Powering all of this requires high-performance, high-availability networks to connect data, machines, vehicles, people and processes – all while protecting the entire ecosystem with multi-layered security.

Every industrial setting is unique - there is no one-size-fits-all solution. That's why the best results often come from working with industrial automation experts who can take a broader, end-to-end view of automation requirements and draw on an ecosystem of experienced partners to integrate the right solutions across an operation or process.

Industrial automation digital maturity model

Because many companies have multiple sites with diverse technologies, systems and standards, and because automation is typically a journey rather than a single initiative, it's helpful to consider it in four progressive maturity stages: connected, integrated, intelligent, automated.

To support your industrial automation journey, this paper provides a detailed look at each of these stages, outlined in the digital maturity model on the following page.

While maturity stages are likely to vary across sites, processes and operational tasks depending on organisational needs, legacy systems and architecture, applying the lens of maturity to any process or operation provides a benchmark to set realistic milestones and goals. It also enables you to understand what measures are required to progress, the services and solutions available, and how to strengthen and embed end-to-end security across your operations.

1. Mckinsey: Australia's automation opportunity.
2. iTWire: Four big workplace trends that will reshape Australia in 2023

Industrial automation
digital maturity model

Start by identifying where the process or operation you want to automate stands and review the summary of requirements. Then examine the corresponding section of this paper to understand more detail.

	Stage 1 Connected	Stage 2 Integrated	Stage 3 Intelligent	Stage 4 Autonomous
Capability	The first stage of automation involves identifying areas for automation potential, installing sensors and actuators or single robots that are not linked in a process in order to digitise data and activities. At this stage organisations also lay the industrial network foundation – a fundamental building block for progressive automation maturity. • Machinery and Fleets securely connected and visible • IoT environmental and people safety monitoring • Remote sensor management • Operational data collection • OT condition monitoring	Converging IT and OT systems is a key step to advanced automation. This is when companies connect relevant IT and OT systems, and collect and analyse data to gain a more comprehensive view of their operations and use monitoring and control systems to automate processes. • Control of machinery and vehicles • Process orchestration for end-to-end efficiencies • Supervisory SCADA systems • Data literacy and aggregation for reporting and compliance	Once IT and OT systems are integrated, companies can start to leverage analytics, AI and Machine Learning to introduce intelligent capabilities like predictive maintenance, adaptive production, quality control, asset tracking, as well as inventory and supply chain management. • Online, actionable decision prompts for management and maintenance • AI and Machine Learning • Subject matter experts interpreting operational data	At this stage companies have automated their manufacturing platforms, optimised supply chains, and introduced sophisticated data analytics to enhance and sometimes automate their decision making. They are now looking at using robotics and robotic process automation. • Fully automated • Sense and manipulate activities in response to external events • Tracking materials, products and workflows for supply chain improvements • Fully integrated Process Control Systems with automated analytical feedback
Intelligence	• Reactive • Operational data informs plans & priorities • Planned maintenance operations	• Proactive • Sensor data securely integrated into applications delivering oversight and alerting • Process analytics informing operational improvements	• Predictive • Improvement and optimisation modelling • Advanced process control techniques	• Adaptive • Operational performance self-optimises in real time
Technology	• Secure 5G/Private 5G • Secure industrial communication networks • Secure connected IoT sensors • Robust, supportable OT network infrastructure	• Edge Compute and data • Integrate OT systems, switchboards, motor control centres, control panels, business systems etc. • Cyber security for OT & IT • Operational data platforms and tools	• Data is aggregated and integrated with company systems – ERP, CRM etc. • Integrated analytics • Digital twins for modelling • Process performance software	• Data flows to automation systems for end-to-end automation and control • AI and Machine Learning optimisation • Digital twins for testing and operational improvements
Assurance	Trusted secure data			

1 Getting connected

Successful automation starts with a plan. Most companies test the water by automating a single process or task that will potentially yield the best outcomes. By implementing it as a proof of value they can refine their approach and demonstrate both feasibility and business potential to the enterprise.

A good place to start is with frequently performed, time-consuming tasks that fall into the category of dull, dirty or dangerous. Automation performs repetitive tasks in high volume faster and more reliably than people, and automated machinery and vehicles can operate with less risk in environments that are hazardous to humans.

Look for processes that require repeatability and controllability and which create substantial value-add. For example, readings for environmental management, video site safety monitoring or repetitive IT and OT system functions.

It's worth evaluating several candidate processes to identify common sequences that can be reused or linked in other automation projects as a discrete step or

task in a future process. Working to a broader vision as you progress with an initial single stream can benefit complementary or parallel processes and avoid a siloed approach. Best practice calls for creating a consistent framework and roadmap for industrial automation in your organisation.

Having made the selection, analyse and optimise your processes before you automate them. A common rule in automation is “never automate a bad process”. You can only effectively automate a process if it happens in the same way every time and if you can design a control system that’s capable of repeating that routine.

Working with an experienced automation engineer will enable you to design processes and decide how to manage exceptions or the need for human oversight or intervention in the process. You also need to understand how automation will change your operations both downstream and upstream, because automating one process may create a ripple effect right across your organisation, impacting other processes and functions from upper management to operations.

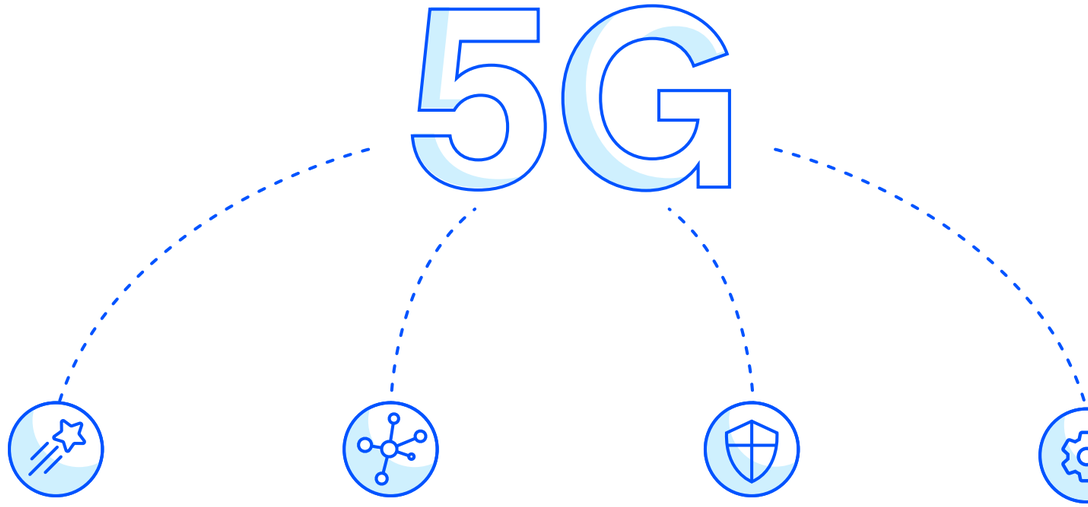
Every task or workflow has a business value and cost. Establishing a pre-automation baseline and then rigorously measuring cost and benefit associated with things like wastage, lost business from poor quality control or inaccuracy and labour as you automate is critical to the success of most automation programs.

“The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency.”

Bill Gates

Why 5G is ideal for industrial automation

5G networks
5G can provide high speeds, low latency and massive capacity making bandwidth-intensive processes, like near real-time data transfer and analysis, augmented reality (AR), virtual reality (VR) possible at a larger scale.



Ultra high-speed and low-latency
Supports near real-time control and monitoring of industrial automation systems

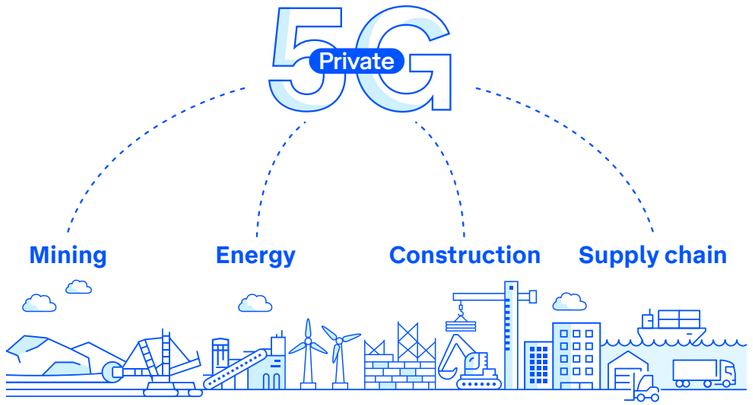
High connection density
More devices can be connected and more data transmitted without causing network congestion

Enhanced reliability and security
Encryption and authentication protect data from cyber threats

Flexibility and scalability
To adapt and customise the network for different industrial automation configurations

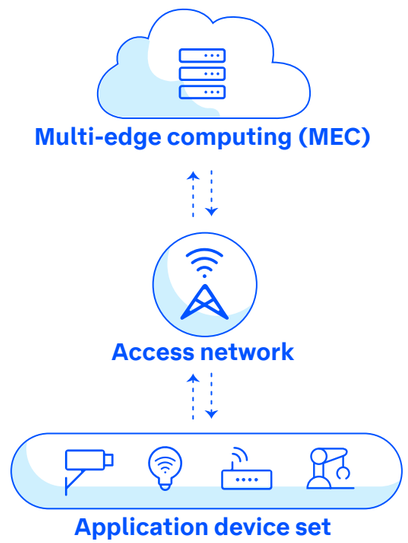
Many of the technologies driving industrial automation, including IoT, robotics, analytics, AI and AR require an evolved network infrastructure that can support the sheer volume of connected and powered devices, the increase in data traffic and stringent requirements around ultra-fast response times and availability.

5G is a fast- evolving network architecture



Private 5G networks

Private 5G networks are designed for exclusive use and can be customised to meet the specific needs of the site with high levels of security, reliability and flexibility.



Multi-access edge computing (MEC)

MEC brings computing resources closer to the edge of the network, allowing for faster and more efficient data processing for industrial automation applications.

5G Network slicing

Network slicing allows organisations to create dedicated network slices for industrial automation applications, with customised performance, security and reliability features.

Next steps

Industrial network site assessment

A great place to start is with an industrial network assessment. For existing operations, Aqura can provide a specialist review, identifying opportunities to optimise and evolve your industrial network to provide better outcomes for your automation objectives. For greenfield sites, the Aqura team is highly experienced in designing, implementing and managing industrial networks that can scale economically as your business requirements evolve. You'll receive a high-level overview of your infrastructure and requirements, technology suitability for your use case(s), analysis of factors such as spectrum availability and congestion and a cost estimate.

Telstra Edge for industrial automation

This Telstra Purple facilitated engagement takes you from industrial automation concept to proof of concept. We'll work with you to design, architect and implement a solution using AWS ruggedised Edge hardware in a distributed cloud environment that enables you to build and run applications on premise, where your data is generated. The solution brings together the power of the Telstra network with AWS's innovative range of DevOps tools and services to advance innovation with low-risk, low-cost experimentation on-premise, where your data is generated.

Designing a network that's fit for automation

Whether your site calls for 4G/5G/LTE, fibre, satellite, mesh or a combination of connectivity, you need to design a high-performance network that is reliable, secure and scalable. Here are some steps to consider.

Identify the automation requirements. Determine the specific requirements of the industrial automation system, including the number and types of devices that will be connected to the network, the amount of data that will be transmitted, expected response times and the level of availability required. Also consider the flexibility required as you reconfigure the layout of your operations.

Choose the appropriate network topology. Select the appropriate network topology based on the automation requirements and the physical layout of the facility. Performance is a key consideration as you will need reliable, assured connectivity across a range of automation devices.

Choose the right network technologies. Different network technologies, whether wired or wireless have their own characteristic strengths and weaknesses and consistently evolve. For example, 5G is a highly flexible technology that offers several advantages making it well-suited for industrial automation networks. These include the ability to support ultra-high bandwidth and extremely low latency, which are important for industrial automation applications that require near real-time control and feedback. 5G also supports massive device density to reliably connect a vast number of new network devices and systems – from sensors and cameras to robots and autonomous vehicles. 5G networks also use advanced technologies, to help maintain signal and reliability, even in challenging environments like factories and warehouses.

Focus on network security. Industrial automation networks must be secured against unauthorised access and cyber-attacks. Implement security measures such as firewalls, intrusion detection systems, encryption and access controls as one critical layer of a holistic end-to-end security approach.

Plan for scalability. Design the network with future growth and scalability in mind. Simplify network design to enable faster deployment and provisioning to cope with the need for additional devices, increased data volumes, and new applications that may be added to the network over time.

Consider long-term manageability. As network architectures become more distributed and complex, specialist expertise will be key to scaling and optimising your network to meet your operational needs. This is particularly the case in environments requiring support for remote devices, applications and systems. Consider a managed service that allows you to focus on core business while experts take care of your network and security.

Work with seasoned experts. Network design professionals understand the unique requirements and challenges of industrial processes and can offer solutions that can bring the greatest value now and in the future. For example, they can help ensure that safety standards are met and risks are minimised. And with technology evolving at a fast pace, network specialists can help you prepare for technological advancements so that automation systems remain effective over time.

How 5G is transforming mining

Discover how advanced LTE and 5G underground mobile technologies support a safer, more sustainable gold mine at Newcrest's Cadia and how their private LTE network is setting the stage for tele-remote and autonomous mining tech at their Lihir gold mine.

Find out more

2 Integrating IT and OT systems

Matt Griffiths, Managing Director, Alliance Automation and Warren Jennings, CTO for Industry at Telstra explain how to embark on successful IT and OT integration.

The integration of information technology (IT) and operational technology (OT) allows companies to collect and analyse data to gain a more comprehensive view of their operations and use monitoring and control systems to automate more complex processes.

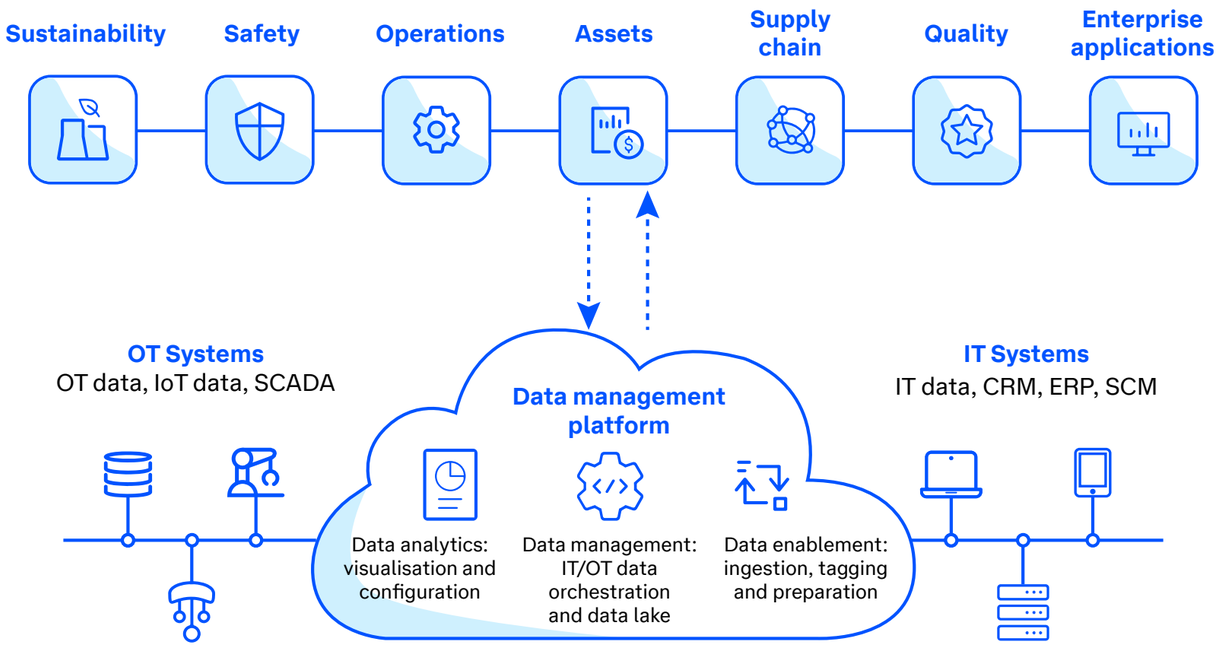
IT systems are typically used for business operations, such as accounting, customer relationship management and supply chain management. OT systems, on the other hand, are used to monitor and control industrial tasks such as manufacturing, energy production and transportation.

The power of industrial automation is typically unlocked when IT systems are used to drive OT systems and when data from OT systems is used to inform IT systems – that is to say – when IT and OT converge. When the two are properly integrated they can combine business processes, insights and controls into a single uniform environment that can help companies to obtain a range of benefits.

These include near real-time monitoring and control of industrial processes to quickly identify and respond to issues, more efficient operations, reducing waste, improving quality, reducing costs and introducing greater agility to respond to market conditions, such as shifts in demand or changes in regulations.

The success of IT/OT convergence is crucial to successful industrial transformation. But typically, OT and IT environments are siloed and often owned by different parts of the business. OT can be a mixture of legacy and modern systems that are geographically dispersed. OT may lack a consistent security framework – and if there is a solid OT security framework, it is seldom aligned with an organisation's IT security framework – creating vulnerabilities as convergence progresses. Historically IT and OT have been designed for different purposes and with different priorities, which usually means they have evolved different architectures and protocols and supporting teams with very different cultures. This creates a range of challenges – from bringing together the teams who manage OT and IT to understanding the competencies needed, as well as finding a way to integrate devices and data, and develop holistic management frameworks with end-to-end cybersecurity.

Applications and Integrated Operations



IT/OT Integration

IT and OT have traditionally been separate functions of the business. Integration brings information from production processes and makes it accessible and controllable at the operations and planning layers of the business.

Next steps

Alliance Automation Asset Pre-Audit

A pre-audit asset assessment provides a cost-effective way to assess your business readiness for an official audit by first identifying weaknesses and vulnerabilities in systems, and areas of non-compliance. We target critical areas that hold the highest risk to the organisation by reviewing documents and observing people and processes. We also create audit trails to critically test effectiveness of controls, and we sample manuals, records and documents that directly relate to audit's objectives. You'll receive a comprehensive report with an asset registrar template and a list of known issues and vulnerabilities to shape your actual asset audit.

Getting started with IT/OT integration

Get expert advice early. IT/OT integration is a complex process with many factors including systems, switchboards, motor control centres, control panels and business systems. You need a partner who can develop a plan, an architecture and a roadmap for integrating IT and OT systems, outlining the sequence of steps to be taken and the timeline for each, taking into account the technical requirements, resource availability and potential risks. Engaging them early helps minimise cost, complexity and delivery time for automation initiatives.

Integration experts can advise you on a range of data acquisition, exchange and processing platforms that collect, aggregate, process, store, correlate and circulate data. They'll also identify the most appropriate integration methods for your company's needs and goals. This could include middleware, APIs, gateways, or other integration tools.

Assess your IT/OT environment. The key to automation is data sharing, and so the first step is to assess the current state of your IT and OT systems and the data they produce and house. Identify the systems and applications in use, as well as existing communication channels or data flows between them. Map this against the goals of the integration project. This could include improving operational efficiency, reducing costs, increasing data visibility or improving decision-making capabilities. It's important to devise a set of KPIs to track these productivity, timeliness, quality or resilience goals so that you can benchmark the impact of your integration project.

Develop an OT asset management plan. Another key task is OT asset management. A well-structured OT asset management plan will enable engineers, administrators and cyber security experts to command tens of thousands or even hundreds of thousands of OT assets by accurately keeping track of asset properties.

Design your architecture. Once you've identified the key data required to achieve your outcomes, the challenge becomes to design an end-state architecture capable of transmitting, processing and maintaining the integrity of very diverse data between systems and devices. Often it may need to support near real-time capture, aggregation processing of a number of critical data sets. When you have a clear picture of what is required, establish a well-defined roadmap of the steps needed to achieve your end-state architecture. Good architecture governance is critical.

Consider edge computing. Edge computing can shorten the time it takes for data to travel from the source to the server and back, reducing latency - potentially improving system performance and enabling some forms of control that are not otherwise possible. This is important for applications that require near real-time response, such as control systems and robotics, predictive maintenance and quality control. By processing data at the edge, companies can detect and respond to issues more quickly, reducing downtime and improving overall system performance. Edge computing can also help improve the security of IT/OT systems by keeping sensitive data local and limiting the amount of data that needs to be transmitted over the network.

Test, evaluate and optimise. Once your solution is designed, the implementation will involve rigorous testing with ongoing monitoring to ensure that integrated systems continue to perform as expected and that any issues are quickly identified and addressed.

How IT/OT integration is improving steel production

Alliance Automation helped to improve production reliability for Liberty Primary Steel by integrating systems and deploying a programmable automation controller which gives them high level control as well as fast and safe stop of all moving equipment. As well as improving production, they can now meet safety integrity levels up to SIL3 (AS 62061) and an emergency-controlled stop (as per AS 60204).

3 Introducing Intelligence

Gideon Ratner, Chief Customer Officer, Quantium Telstra and Warren Jennings, CTO for Industry at Telstra provide insights on using analytics to obtain the full benefits of automation.

Once IT and OT systems are integrated, it's possible to leverage analytics, AI and Machine Learning to introduce intelligent capabilities like predictive maintenance, quality control and asset tracking, as well as inventory and supply chain management.

Industrial intelligence starts with ensuring key data is digitised and aggregated from devices, systems, machines, databases, sensors and vehicles. It also starts with ensuring that data is actively managed from its source. Once this data is standardised and exposed in usable format, it can then be interpreted and used as the basis for models and analysis to drive decisions and automation.

For example, AI techniques such as ML algorithms can be applied to identify patterns and anomalies, predict future outcomes to optimise performance, inventory levels and shipping routes, while reducing waste, energy consumption and optimising delivery times.

Predictive maintenance algorithms can be used to identify when equipment is likely to fail and schedule maintenance before a breakdown occurs. This often reduces downtime and cost associated with unnecessary maintenance.

Consolidated data from IoT sensors can be used to improve decision-making, optimise performance and, when integrated with reporting software, it can help to automate safety and environmental management.

Some of the uses in industrial settings include:

- Helping transport and supply chain organisations gain better visibility into the coordination, condition and usage of assets to guide short-term repairs, route optimisation and long-term planning for asset replacement and safety.
- Helping mining, shipping and construction companies to minimise plant and asset downtime and maximise equipment utilisation.
- Helping oil, gas and electricity utilities to optimise industrial equipment inspections, make damage assessments and handle inventory monitoring and distribution.

Introducing Intelligence

Data Management Platform with integrated analytics capabilities.

Applications
Analytics, BI, Visualisation, Reporting

Data Security and Governance
Data logging, Classification, Authentication, Alerting

Data Storage
Cloud, On premises

Data Acquisition
Sensors, ERP, Excel, Video, Operations Data

Next steps

Quantium 1-day data science workshop

This one-day consulting engagement with Quantium will provide insights into the world of data science and advice on how to advance your company's data analytics maturity. You'll learn about best practice and relevant use cases, as well as where your organisation sits on the data science maturity curve. We will also workshop an initial view of your priority initiatives.

Telstra Purple Data Assessments

Telstra Purple offers various data-led assessments, including data-led discovery, data engineering PoCs, machine learning PoCs, and machine learning accelerators.

Getting started with analytics

Find partners you can trust. While analytics, AI and data modelling can optimise automation, few companies have the breadth of technical skills, experience or the methodologies to deploy and work with these tools effectively. Unless you're sure you do, it's a good idea to call on professional help for the best results as you work through the following steps.

Build your strategy. A great place to start is by identifying the production, processing or handling processes and activities where you need to change the game. Focus on understanding the critical decisions where data from your OT should drive your business processes or where you need your OT environment to directly respond to decisions.

Start, learn and expand. Choose a candidate process where analytical decisioning will yield measurable benefit and focus on a manageable slice of that (for example one individual production line). Understand the critical decisions to be made and identify the key data underpinning those decisions. Critically examine the data: What is its quality? Is it actively owned and managed? Is it highly available? And in a timely manner? Start with the smallest well-managed data set you can and make the analytics approach and integration as simple as possible.

Measure the benefits and impact on other parts of your organisation. Take learnings around your analytics approach, integration with IT governance, maintainability, security and auditability. Use these to iterate your strategy and build your implementation roadmap.

Scale. As you iterate and expand you'll build a consistent pragmatic framework for data ingestion, storage, management and analysis. You'll understand shortcomings and establish a targeted investment program to improving data quality, access controls, adopt standards, enhance auditability and management. You will also be able to establish the right data governance model for your organisation, which is critical to establish appropriate protections, access controls and audit trails to help ensure data security and compliance with industry regulations. Your organisation will gain a good understanding of the tools and platforms it needs.

Importantly, your organisation will obtain a much better understanding of your requirements for data management tools, data platforms and analytical software to underpin your intelligent automation journey. A common issue in many intelligent automation programs is jumping to technology decisions too early - locking organisations into inappropriate tools and wasting valuable time and resources.

Bis are using data to improve driver safety

Telstra Purple helped Bis to unify the data from multiple IoT devices, across many different languages and systems in order to analyse driver fatigue ratings, journey times, and understand the consequences of actions. With a better understanding of people and their roles they are now optimising shift rosters.

Find out more

4 Automating your environment

Once companies have gained confidence in using industrial automation to optimise manufacturing platforms, supply chains and business processes, they can start to reimagine business operating models and strategic plans with automation as a central focus.

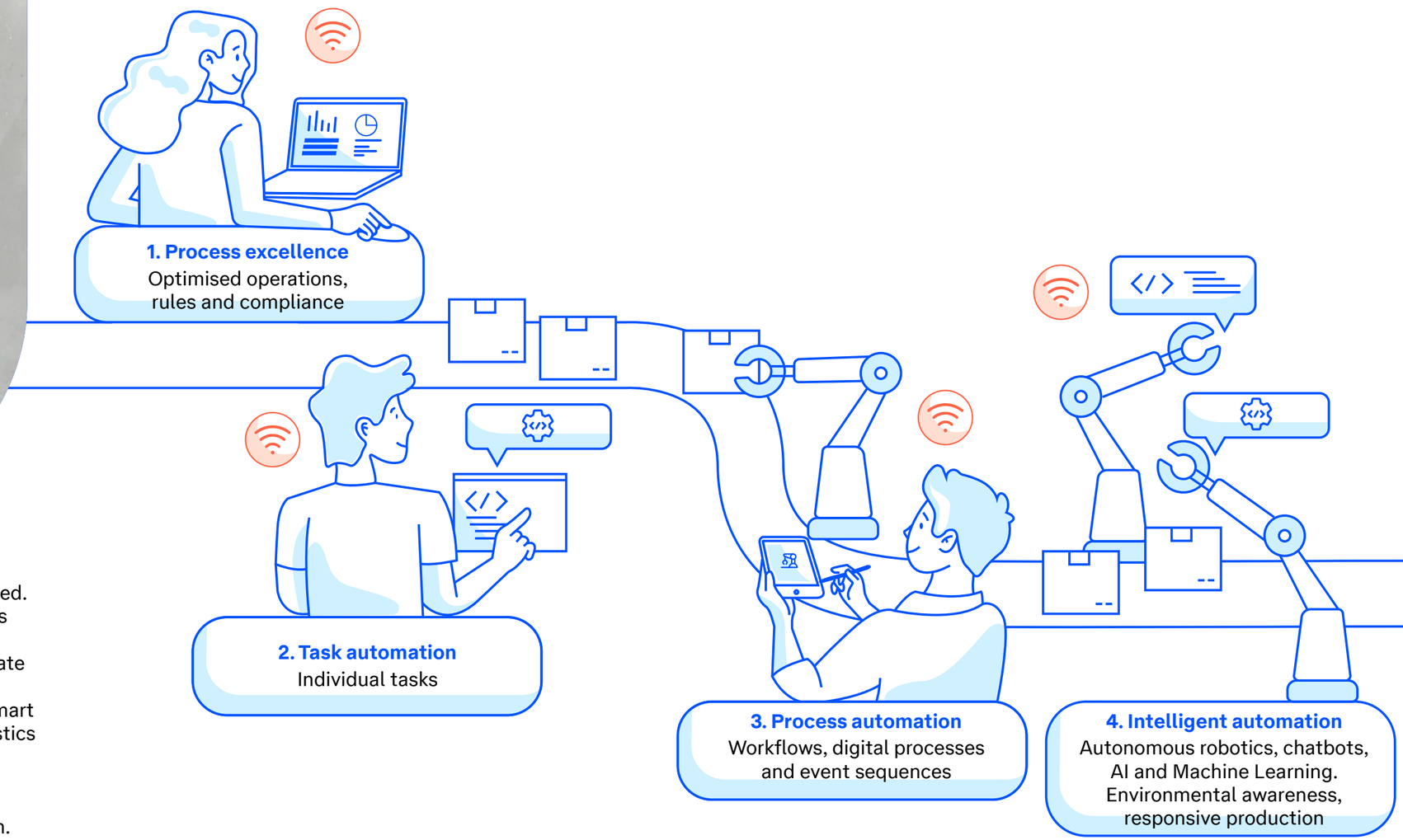
By introducing advanced technologies such as automated mobile robots, guided vehicles, robotic process automation, artificial intelligence and machine learning, organisations can increase the automation of business processes (production processes, workflows, marketing etc.) to a point where almost any repetitive task can be transformed.

The technology can even be used to discover which other processes are amenable to automation and assist with many of the tasks to automate them.

Automation at this level benefits both staff and the business. Humans become supervisors rather than operators - spending their valuable time managing exceptions rather than the day-to-day. Personal safety improves through less exposure to hazardous environments or dangerous processes. There is also the potential to improve employee wellbeing and mental health by assigning more creative roles in the place of repetitive and dull tasks.

The journey to automation

Moving from task automation towards hyperautomation is a progressive journey.



From a business perspective, output or product quality improves when each task or unit of production is standardised. Automated processes better adhere to design specifications or protocols within tight tolerances and they offer superior repeatability. They are also typically faster with a reduced rate of error. And once an entire process is automated it can run 24/7 or adopt more dynamic schedules to meet demand. Smart devices and automated machinery can also run self-diagnostics and alert human operators to potential malfunctions, streamlining maintenance and repair. The resulting preventative maintenance and faster breakdown response times make machinery and fleets less expensive to maintain.

Ultimately, an automation culture can also open new opportunities, allowing your organisation to create value from new product and service streams that would not be possible otherwise.

Next steps

Purple Strategy engagement
This offering helps you define challenges, understand your most important business opportunities, align their people around an agreed approach and devise a strategy to execute. Experts will work with you to help you obtain clarity on business value, vision and metrics that matter. The engagement will surface new ideas and potential paths forward, as well as their relative value, to create an agreed roadmap with prioritised actions.

Purple Labs 5-day design sprint
Working with Purple Labs over a 5-day design sprint, you'll have the opportunity to rapidly validate ideas and de-risk new projects. The process includes research, problem definition, articulation of the future state, defining a plan to move forward, and embedding a delivery team to build your solution.

Getting started with automation

Seek expert advice. Automating an entire business environment requires careful planning, investment, and collaboration across different departments and functions. From a technical perspective, it is not based on one single technology but on integrating and orchestrating multiple technologies. It's also about creating a culture of continuous measurement, monitoring and optimisation in your organisation. The range of technologies, process changes and human change management involved can be significant with many potential potholes. The right advice can help you plot the right path for your organisation.

Start with Business Process Management (BPM). Use this methodology for designing, implementing, and managing business processes to model, automate and optimise them. This requires a comprehensive understanding of the processes in your business, where they intersect and how they impact each other.

Consider deploying Robotic Process Automation (RPA) which is a light-touch approach that allows you to automate repetitive, rule-based tasks that are typically performed by humans. RPA bots can be programmed to mimic human actions, such as opening applications, entering data and performing calculations. Often this programming is learned by bots shadowing the humans who currently conduct these tasks.

Invest in Artificial Intelligence (AI). Technologies such as machine learning and natural language processing enable machines to learn from and make predictions or decisions based on a wide range of data. Evaluate the opportunities for Intelligent Process Automation which combines RPA with AI to enable end-to-end automation of complex business processes that involve unstructured data, decision-making and multiple applications.

Investigate the use of Chatbots. These programmable entities use natural language processing (NLP) and AI to interact with humans through text or voice to automate customer service, sales, and support processes, providing quick, personalised responses. Evolving approaches such as Large Language Models (LLMs) are creating step changes in the capabilities of chatbots.

Are Cobots right for you? In many organisations, full automation is not warranted or economically feasible. In these environments, assistive automation such as cobots can have a huge impact. Cobots are a type of robot designed to work alongside humans in a shared workspace to perform tasks like assembly, packaging, inspection, and machine tending. Unlike traditional industrial robots, which are often designed for specific tasks and require significant reprogramming to adapt to new tasks, cobots can be easily reprogrammed and redeployed for new tasks.

Evolution Mining are applying process controls systems to Mt. Carlton Gold Mine

Alliance Automation supplied the Process Control System (PCS) for the processing plant and all associated infrastructure. This comprised design, development and testing of PCS in the following areas: mining workshop, HV, Crushing, Grinding, Flotation, Reagents, Concentrate and administration. The complete PCS design package included: design specifications, control and communication panel general arrangements, schematics, terminations and schedules; ITPs and commissioning plans, along with on-site commissioning.

Find out more

5 Securing an IT/ OT environment

Matt Griffiths, Managing Director, Alliance Automation and Warren Jennings, CTO for Industry at Telstra describe the key considerations when securing IT/OT environments.

The convergence of IT and OT platforms has expanded the attack surface through the connection of sensors, machines and devices and increased the risk of cyber exploitation of control systems.

Converged IT/OT systems can be vulnerable to attack due to a number of factors, including outdated hardware and software, poor network security, lack of system segmentation and insufficient access controls.

Operational technology environments can be complex, geographically dispersed and consist of a mixture of current and legacy systems that may not have been updated to meet modern cybersecurity standards.

Traditionally, OT systems have operated separately from IT environments and were rarely connected to IT networks and the Internet. Their security was designed to cater to the specific security requirements of the equipment or machine. This results in vulnerabilities that can be exploited to gain unauthorised access to the system, steal sensitive data, disrupt operations and cause physical damage to equipment.

The implications of OT system attacks can be severe. In industrial environments, attacks can lead to production downtime, equipment damage, and even safety incidents.

IT/OT cybersecurity domains

Security governance

Audit your environment and develop policies, procedures and training with incident response and governance.

Perimeter security

Monitor, authorise and control traffic between the ICS network and the company IT network.

Staff training

Issue training policies and response procedures with regular updates.

ICS network

Segment the network and create a secure, reliable layer for critical communications.

Critical site security

Restrict access to authorised personnel, using multi-factor authentication and CCTV.

Supply chain security

Set up contracts with supply chain partners to mandate security standards and incident response handling.

24/7/365 monitoring

Set up Intrusion Detection Systems and configure Security Incident and Event Monitoring with proactive alerting and incident response plans.

Server and device security

Harden field devices, whitelist applications, configure encryption and security and embed patching and vulnerability management.

For example, an attack on a power plant or water treatment facility could result in a widespread outage or contamination of the water supply.

Attacks on IT systems can lead to theft of intellectual property, loss of customer data or sensitive commercial data, and damage to the company's reputation as well as having financial consequences. The cost of recovering from an attack can be significant and there may be regulatory fines or other penalties.

Increasingly, organisations offering cybersecurity insurance to help mitigate these impacts require their customers to implement strong cybersecurity regimes as a condition of coverage.

Protecting your environment

When designing security measures for industrial automation, it's important to factor in the fundamental differences between IT and OT technology.

IT systems communicate over known protocols like HTTP, use shared environments like the cloud or virtualised servers and deploy security controls like firewalls and antivirus. OT systems, on the other hand, communicate over industrial protocols like Modbus, SCADA, Ethernet/IP and Profinet. They use different programming paradigms and sometimes have highly constrained computing capability. They are often "headless" and provide few, if any, security and access controls.

Historically, OT incidents may be significantly more damaging, but IT has more vectors for compromise due to the sheer number of ingress points and software complexity.

IT and OT systems have been designed according to different priorities. For IT, the key concern has been confidentiality of company IP and data. IT security frameworks use a paradigm of frequent, often centrally managed patching - with failed patches easily "backed-out".

Operational technologies/industrial control systems (OT/ICS) have been designed for maximum availability and safety. Patching can require production shutdowns and failed patches can be difficult to reverse.

OT systems and assets usually have a much longer life cycle and can be decades-old, with few or no updates issued by system vendors (If those vendors still exist). So known and exploited vulnerabilities are unaddressed for much longer.

Implementing Security by Design

Converged IT/OT systems and processes should be designed by integrating security measures into every stage of the development process, from design to deployment and maintenance. There are several key principles of security by design, including:

- Conduct a risk assessment to identify critical assets, potential attack vectors, and the likelihood and impact of different types of attacks.
- Segment the OT network to reduce the attack surface and limit the impact of a potential breach. This involves dividing the network into smaller, isolated segments that are easier to monitor and secure.
- Implement appropriate access controls, such as two-factor authentication, and limit user privileges to only those that are necessary.
- Regularly monitor OT systems by implementing intrusion detection systems (IDS) and security information and event management (SIEM) systems. These help detect and respond to potential attacks, as well as proactively updating and patching the system to address known vulnerabilities and reduce the risk of attacks.

Next steps

Purple IT/OT Cyber Assessment
Telstra Purple will assess your assets to identify risks, threats and vulnerabilities to your OT environment. You'll receive a clear report on the security status of your assets along with mitigation recommendations to close security gaps based on a "secure by design" approach to cyber resilient architecture. We recommend how you can simplify threat detection and make systems difficult to compromise, yet simple to operate.

Getting started with a security architecture

Work with IT/OT security experts. Given the complexity of IT/OT security management, most companies require consultative technology partners with expertise across networks, connectivity, cloud and IoT to implement effective security strategy and controls.

For organisations who do have the necessary security and detection techniques, it's essential to have proactive monitoring and an incident response capability you can call on.

Even for organisations who have a well-resourced and highly capable security team, an essential part of good cybersecurity practice is to get regular independent reviews of your security frameworks and processes.

Audit your assets. Safeguarding your environment begins with understanding what each IT and OT component does, how they differ and how they interact, and then developing a comprehensive cybersecurity strategy.

Assemble your team. You may need to create a cross-functional cybersecurity unit that straddles IT and OT security drawing on different teams across the business. Working with an experienced partner, this team can carry out a comprehensive security assessment of your industrial automation ecosystem, including hardware, software, network and data and then adopt a risk-based approach, identifying your most critical assets and vulnerabilities and prioritising security efforts accordingly.

Design a security framework. You can then work with IT/OT security experts to implement a security framework that defines the policies, standards and procedures for securing your ecosystem. This may involve adopting industry best practices such as SASE, the Essential 8, ISA/IEC 62443 or the NIST Cybersecurity Framework.

Deploy security measures. Experts can then work with you to secure the hardware components of the industrial automation system by implementing physical security measures such as access controls, CCTV and intrusion detection systems.

Safeguard the network. You'll also need to secure the network infrastructure using firewalls, intrusion detection/prevention systems and strong authentication mechanisms. This could involve isolating critical systems from non-critical systems and using virtual private networks (VPNs) for remote access.

AI techniques can help to detect and stop new forms of attack by Identifying and analysing unusual traffic patterns.

Protect the software. The software components are equally important. These can be protected by implementing secure coding practices, using secure protocols for communication and maintaining regular patches and updates.

Monitor and update. Once your environment is secured, you'll need continuous monitoring using intrusion detection systems, log management and security information and event management (SIEM) systems. Visibility is critical, so opting for the services of a Security Operations Centre (SOC) that offers 24/7 proactive monitoring and agreed response times is essential.

Mirvac moved from legacy perimeter security to a holistic cloud platform
Mirvac enhanced their security posture and laid a foundation for the future with Security Incident and Threat Prevention services, distributed denial of service (DDoS) protection, data protection, access control systems, content filtering and more – all augmented by security audits.

Find out more

Telstra industrial automation

Every industrial setting is unique, so it’s critically important to work with experts who understand automation and have the capabilities and expertise to deliver. Through strategic acquisitions and partnerships Telstra combines professional expertise, high-speed industrial network design, IT and OT integration, control systems and advanced analytics to design and deploy industrial solutions and protect them with end-to-end cybersecurity. With over 2,000 + expert consultants, we are ready to help you take the next step.

Telstra Purple

AQURA A Telstra Purple Company

alliance automation A Telstra Purple Company

quantium

telstra.com.au/industrial-automation